PURPLE GRIFFON
The IT Service Management Training & Consultancy Specialists

Course Title: BCS Practitioner in Information Risk Management	**Course Duration**: 5.0 Days
Exam: Included	**Exam Type**: Proctored Exam
Qualification: BCS Practitioner Certificate in Information Risk Management	

Course Syllabus

The syllabus for BCS Practitioner in Information Risk Management course is as follows:

1. The concepts and framework of information risk management

1.1. Explain the need for information risk management.

1.2. Explain the context of risk in organisations.

2. Information risk management fundamentals

2.1. Explain the fundamentals of information security.

2.2. Explain information risk management standards and good practice guides.

2.3. Explain the process of information risk management.

2.4. Explain information risk terms and definitions.

3. Establishing an information risk management programme

3.1. Understand the requirements of an information risk management programme.

3.2. Explain the development of a strategic approach to information risk management.

3.3. Explain the principles of information classification.

4. Risk identification

4.1. Describe the process to identify information assets.

4.2. Conduct a business impact analysis.

4.3. Conduct a threat and vulnerability assessment.

5. Risk assessment

5.1. Undertake a risk analysis.

5.2. Conduct risk evaluation.

6. Risk treatment

6.1. Explain risk treatment options, controls and processes.

6.2. Explain the use of a risk treatment plan.

7. Monitor and review

7.1. Explain information risk monitoring.

7.2. Undertake an information risk review.

8. Presenting risks and business case

8.1. Report and present the progress of a risk management programme.

8.2. Present a business case

Course Overview

The BCS Practitioner in Information Risk Management course equips professionals with the skills needed to identify, assess, and mitigate risks associated with information security. This course delves into core concepts, including risk assessment methodologies, control selection, and the integration of risk management into broader business strategies.

Information risk management is crucial because it ensures that organisations protect their sensitive data from breaches, leaks, and other cyber threats. Poorly managed risks can lead to significant financial losses, reputational damage, and legal penalties. By understanding potential risks and putting effective safeguards in place, businesses can maintain their operational integrity and protect both client and internal data. The course provides practical tools for handling real-world challenges, giving professionals the confidence to manage and reduce risk efficiently.

Course Learning Outcomes

Upon completion of this module, candidates will be able to demonstrate:

- Knowledge and understanding of information risk management principles and techniques.
- An understanding of how the management of information risk will bring about significant business benefits.
- An understanding of how to explain and make full use of information risk management terminology.
- A practical understanding of how to conduct threat and vulnerability assessments, business impact analyses and risk assessments.
- A practical understanding of the principles of controls and risk treatment.
- A practical understanding of the use of information classification schemes.
- A practical understanding of how to present the results in a format which will form the basis of a business case for a risk treatment plan.

Audience

This qualification has been designed for Information Risk Managers and all those who have responsibility for managing information, whether in the public or the private sector.

Entry-Level Requirements

There are no mandatory requirements to undertake this qualification, although candidates will need a good standard of written English. It will be advantageous to have an understanding of the laws that affect information risk management such as the Data Protection or Freedom of Information regulation before the course.

Recommended Reading

We recommend reading articles on information security management, information risk management, GDPR legislation, and other relevant topics.

What's Included

Course Materials (E-book)

Exam included

Exam Information

The examination is a closed cook, multiple choice, scenario-based online exam

Duration: 90 min

Supervised: Yes

Passmark: 39/60 (65%)

What's Next

If you see yourself with gaps in your knowledge base we recommend:

ITIL Foundation (For basic ITSM knowledge)

ITAM Foundation (For internal information management)

Additional Information

At its core, IRM involves understanding the value of the information, the vulnerabilities it may have, and the likelihood and impact of any risks that could exploit these weaknesses. Key risks include unauthorised access, data breaches, and loss of data integrity. Organisations prioritise these risks based on potential impact and likelihood, and then implement measures to minimise or eliminate them.

One of the most effective ways to manage information risk is through a combination of security controls, such as encryption, firewalls, and regular audits. Additionally, employee awareness and training are crucial in mitigating risks, as human error is often a significant factor in data breaches.

IRM is not a one-time task; it requires ongoing monitoring and updating to keep pace with new threats and changes in technology. Organisations often use risk management frameworks, such as ISO/IEC 27001, to guide their IRM practices and ensure a structured approach.

By focusing on prevention, detection, and response, information risk management helps protect sensitive data and ensures that organisations can maintain their operations with minimal disruption.